DIB-VDP PILOT FAQ

Q1:
Can we include a range of IP for scope?
A1: Yes.
Q2:
How are researchers selected?
A2:
The program is open for any security researcher on HackerOne to participate.
Q3:
Can anyone register with HackerOne to be a researcher?
A3:
Yes, all researchers register with HackerOne.
Q4:
Where is the "Scope and Asset List" form dropdown categories from?
A4:
The available categories are from the DoD VDP Vulnerability Report Management Network (VRMN), however you can type in additional asset types that will be reviewed by the DIB-VDP tech team.
Q5:
Does participation in this program assist a company in preparing for CMMC accreditation?
A5:
Answer varies depending upon each company participation and vulnerabilities. There are benefits but DIB-VDP does not report participation to any other organizations or agencies.
Q6:
If a participant's whole environment (say as identified by companyname.com domain) is approved to process CUI, but parts of it do NOT process CUI, can the participant include the full environment to be in scope?
A6:
Yes. As long as it is a part of a DoD covered network.
Q7:
Can we expect any social engineering attacks via email (phishing) from pilot researchers?
A7:
No, all social engineering attacks are prohibited from DIB-VDP pilot and the DoD VDP.
Q8:
Can companies request U.S. Citizen Researchers only?
A8:
No. Crowd-sourced white-hat researchers are globally based.
Q9:
Understanding that the researchers are provided by HackerOne, but are the researchers vetted prior to signing up and accessing company information? How do we know they aren't nation-state sponsored researchers?
A9:
No, researchers are not vetted prior to signing up to HackerOne. The only requirement is that researchers must have a HackerOne account and be able to discover, test, and report vulnerabilities in accordance to the posted policy and scope. The researchers are testing publicly accessible assets and reporting vulnerabilities for the system owners to mitigate. DIB-VDP pilot researchers are not "employed" by HackerOne.

DIB-VDP PILOT FAQ

Q10:
Will you acknowledge (with each company) when they have successfully submitted the needed materials and are approved to join the DIB-VDP Pilot?

A10:
Yes, you will receive a congratulatory email after the signed documentation has been received and reviewed. We will supply a DIB VRMN account for your company.

Q11:
If a security notification is sent from one of our security information systems (SIEM) due to the vulnerability assessments what is the process for determining if the source is through a VDP or some other security event?

A11:
Companies will reach out to us via Slack with concerns and VIP DIB will investigate issues with a quick turnaround time.

Q12:
For those of us using mostly cloud solutions, would our endpoints be the only assets we could list?

A12:
Yes if Cloud is owned and operated by companies.

Q13:
If our organization, has features configured to block source IP's found attempting to use known vulnerabilities, will that negatively impact our ability to participate?

A13:
No. That is not impactful.

Q14:
If a vulnerability is found, will suggested mitigation/remediation steps be indicated in the reports? Or is that the complete responsibility of the participant?

A14:
We will provide suggested mitigation and will be available to provide additional information as needed.

Q15:
Is there a status for the participant to state that we are working on remediation? There could be some instances that remediation may be complicated a take a while to complete.

A15:
Yes, the Plan of Action and Milestones (POAM) box is available to capture that information.

Q16:
Does the team offer more mitigation/help should the 'suggested' solution not work?

A16:
Yes. We will be available to mitigate and test via slack, email, or phone call.

Q17:
In the participant scope document can you elaborate on the "type" options: misconfiguration, Radio Frequency (RF), and Sensitive Information Exposure?

A17:
Type: these are standard categories that have been reported to the DOD VDP, you can type in additional categories into the Scope and Asset List dropdown field.

DIB-VDP PILOT FAQ

Q18:

Following up on the Cloud Service Provider question, is it possible to have written permission from the cloud provider (e.g. customer's tenant in M365), so we can put into scope?

A18:

Case by case basis depending on companies’ relationship with Cloud Provider.

Q19:

Any future plans to incorporate additional services such social engineering tests, routine vulnerability scanning, etc.?

A19:

Not at this time within the DIB-VDP Pilot.

Q20:

What happens if a risk is accepted as is (un-mitigated). Does that jeopardize a relationship somehow?

A20:

If the risk is accepted by the company (in the POAM field) it will be annotated in DIB-VRMN and the report will be closed out. It will not jeopardize the relationship or eligibility to participate in the pilot.

Q21:

Can you talk more about a researcher’s timeframe? How do we know when it starts and when we're done?

A21:

Researchers will have test as long as there are assets available in scope. DIB VDP Pilot mitigation schedule is based on report severity ratings: low level findings is 60 days, medium level findings are 21 days, and high/ critical findings are a 7 day turn around.

Q22:

Per the discussion on the Scope and Asset List if we are using a cloud based system like google workspace can we include them?

A22:

If it is a cloud based system that you do not own then we will not be able to include them in the scope unless there is written consent from the cloud system owner.

Q23:

Is there a plan for DIB-VDP to be included in the new SPRS scoring requirement?

A23:

Not at this time but could be foreseeable in the future.

Q24:

Is there a recording of this session?

A24:

This session is being recorded however all attendee identities will be removed before posting.

Q25:

If we have further questions later what is the contact email?

A25:

Yes, please reach out to DIB-VDP@dc3.mil.